The concept of data protection law

Poster · January 2021

DOI: 10.5281/zenodo.3968996

Max von Grafenstein
Einstein Center Digital Future

The concept of data protection law

Controlling informational risks through (not to) the right to data protection

BACKGROUND

Harm-based vs risk-based approaches of protection

In liberal legal systems, laws usually apply a reactive harm-based approach: if harm occurs, the responsible person must restore the original state.

However, in certain situations, laws apply a proactive risk-based approach: they seek to prevent harm before it may occur.

GENERAL REASONS FOR A RISK-BASED APPROACH

A risk-based approach may be preferable, for example, if harm cannot be restored (e.g. in the case of death)...

... or if it is difficult to determine, reactively, which single action has caused the harm (e.g. in the case of environmental pollution).

REASONS FOR RISK-BASED APPROACH REGARDING PERSONAL INFORMATION

The same idea applies to personal information: Once somebody knows something about another one, it is impossible to erase that information...

... and it is difficult to prove afterwards whether this information has been passed on and abused (e.g. by false friends, insurance companies, etc.).

INFORMATIONAL POWER ASYMMETRY AS THRESHOLD FOR LEGAL PROTECTION

The **ECHR** affirms protection only if personal information is *systematically and permanently* stored (not protection of information per se).

The **BVerfG*** sees the special risk in the *automated* processing (i.e. access data instantly and globally, create vast profiles and repurpose the data).

Against this background, how will the ECJ assess data processing risks?

* German Constitutional Court

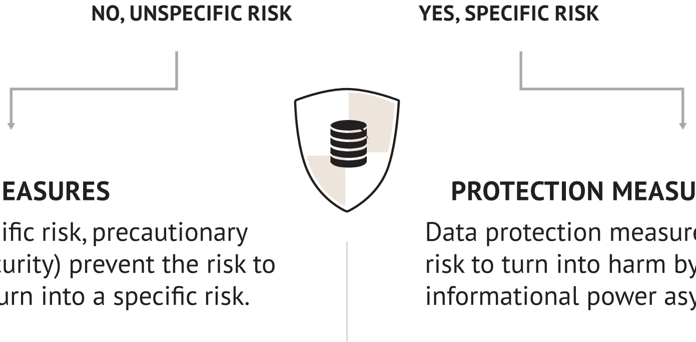
DATA PROTECTION RISK ASSESSMENT

From reason to risk to harm: protecting individual autonomy

?
DATA PROCESSING
CAUSALITY CHAIN
HARM

When regulating risks in general, there are two decisive questions: How likely does a certain reason (the processing of personal data) cause harm to an individual (a data subject). And what kind of harm shall be avoided by implementing (data) protection measures?

Given the data, purpose and processing context, is the risk likely to turn into harm?



PRECAUTIONARY MEASURES

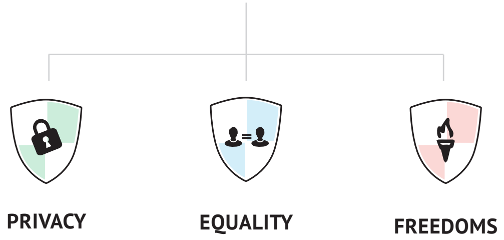
In case of an unspecific risk, precautionary measures (e.g. IT security) prevent the risk to get more likely, i.e. turn into a specific risk.

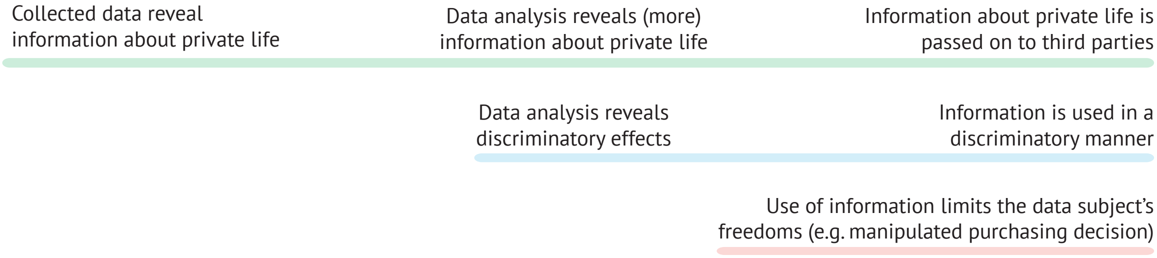
PROTECTION MEASURES

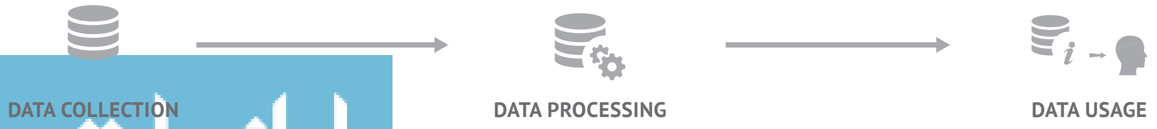
Data protection measures prevent a specific risk to turn into harm by re-balancing the informational power asymmetry.

What is the harm that data protection measures shall prevent?

Data protection law prevents, across varying contexts, data processing risks to turn into harm to individual autonomy (more precisely, protects the data subjects' autonomous exercise of all their fundamental rights, such as to privacy, freedom, and equality).




Collected data reveal information about private life
Data analysis reveals (more) information about private life
Information about private life is passed on to third parties
Data analysis reveals discriminatory effects
Information is used in a discriminatory manner
Use of information limits the data subject's freedoms (e.g. manipulated purchasing decision)


DATA COLLECTION
DATA PROCESSING
DATA USAGE